HOCHSCHULE
MITTWEIDA
UNIVERSITY OF
APPLIED SCIENCES

BACHELORARBEIT

Herr
Pierre Herzog

Manipulation: Eine Breitenanalyse am Beispiel Online-Voting durch Einzelne oder Gruppen

2012

Fakultät: Medien

BACHELORARBEIT

Manipulation: Eine Breitenanalyse am Beispiel Online-Voting durch Einzelne oder Gruppen

Autor:
Pierre Herzog

Studiengang:
Medientechnik

Seminargruppe:
MT09wD-B

Erstprüfer:
Prof. Dr.-Ing. Robert J. Wierzbicki

Zweitprüfer:
Dipl.-Ing. Sieglinde Klimant

Einreichung:
23.07.2012

Faculty of Media

BACHELOR THESIS

Manipulation: a Wide Analysis Using the Example of Online-Voting by Individuals or Groups

author:
Pierre Herzog

course of studies:
Media Technology

seminar group:
MT09wD-B

first examiner:
Prof. Dr.-Ing. Robert J. Wierzbicki

second examiner:
Dipl.-Ing. Sieglinde Klimant

submission:
23.07.2012

Bibliografische Angaben

Herzog, Pierre

Manipulation: Eine Breitenanalyse am Beispiel Online-Voting durch Einzelne oder Gruppen

Manipulation: a Wide Analysis using the Example of Online-Voting by Individuals or Groups

43 Seiten, Hochschule Mittweida, University of Applied Sciences,
Fakultät Medien, Bachelorarbeit, 2012

Referat

Die Macht der Manipulation ist sehr vielseitig, da sie in die Bereiche der Psychologie, Soziologie sowie Politik eingreift. In der heutigen Zeit ist die weltweite Vernetzung und die Interaktion über das Internet ein wesentlicher Bestandteil der Gesellschaft. Doch wie sicher sind unsere Aktionen in der Onlinewelt? Diese Arbeit untersucht die Möglichkeiten der Manipulation am Beispiel des Online-Votings.

Anhand der Gegenüberstellung von Manipulation als Einzelner oder als Gruppe werden Praxisbeispiele und theoretische Aspekte untersucht. Manipulationsmethodiken werden evaluiert und entsprechende Gegenmaßnahmen aufgezeigt, um diese abschließend zu kategorisieren und zu bewerten.

Inhaltsverzeichnis

Abkürzungsverzeichnis

CBSE Computer Based Social Engineering

CAPTCHA Completely Automated Public Turing test to tell Computers and Humans Apart

DDoS Distributed Denial of Service

DGOF Deutsche Gesellschaft für Online-Forschung e.V.

DoS Denial of Service

HBSE Human Based Social Engineering

HTTP Hypertext Transfer Protocol

IP Internet Protocol

IRC Internet Relay Chat

IT Information Technology

Loic Low Orbit Ion Cannon

OCR Optical Character Recognition

PR Public Relations

RSE Reverse Social Engineering

RSS Rich Site Summary

URL Uniform Resource Locator

VPN Virtual Private Network

Abbildungsverzeichnis

Tabellenverzeichnis

1 Einleitung

„Manipulation ist ein uraltes Mittel der Beeinflussung. Sie wurde seit je von allen Kulturen bis zum heutigen Tag angewendet. Bei der Manipulation geht es um bewusste oder unbewusste Lenkung. Manipulierte Darstellungen basieren auf eigenen Zielvorstellungen.“[1] Der Schweizer Autor von Fachbüchern und Fachbeiträgen im Kommunikationsbereich Marcus Knill beschreibt in seinem Artikel „Beeinflussung-Manipulation-Propaganda“ den interdisziplinären Charakter der Manipulation, da diese in die Bereiche der Psychologie, Soziologie sowie Politik eingreift. Der Manipulationsbegriff umfasst etymologisch ein weites Spektrum aus den genannten Disziplinen, so dass für die vorliegende Arbeit dessen Methodik und dessen Auswirkungen auf Medien im Bereich des Online-Voting analysiert werden. Bei Online-Votings handelt es sich um internetbasierte Abstimmungen, welche selbst zum Ziel haben aus mehreren Vorschlägen ein repräsentatives Ergebnis über den favorisierten Endvorschlag zu erreichen. Die Teilnahme an einer Abstimmung unterliegt bestimmten Kriterien, welche je Abstimmung variieren können und bestimmte Benutzergruppen ein- oder ausschließen. Durch Anwendung der Manipulation auf Online-Votings ergibt sich folgende Problemstellung.

1.1 Problemstellung

Das Ziel eines repräsentativen Ergebnisses ist gefährdet durch Manipulation. Diese bewirkt, dass das Ergebnis verfälscht beziehungsweise das Nutzerverhalten durch die interdisziplinäre Ausrichtung des Manipulationsbegriffes psychologisch beeinflusst wird und das Ergebnis seine Echtheit verlieren kann.

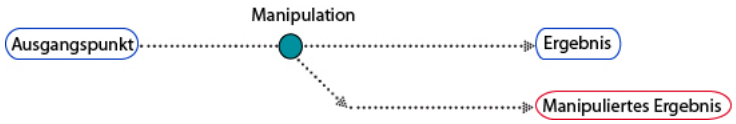


Abbildung 1: Wirkung der Manipulation[2]

Durch den Einsatz von Manipulation wird der Standardablauf gestört, weicht vom Normalverlauf ab und führt zu einem anderen Ergebnis. Es gibt eine Vielzahl an Methodiken von diesem Standardablauf (Standardszenario) durch Manipulation abzuweichen, woraus sich die folgende Zielstellung der Arbeit ergibt.

[1] Knill 2009, http://www.rhetorik.ch/Beeinflussen/Beeinflussen.html, 02.05.12
[2] Darstellung des Autors

1.2 Zielstellung

Ziel der Arbeit ist es, Methodiken der Manipulation im Internet sowie geeignete Gegenmaßnahmen aufzuzeigen, den Versuch zu unternehmen, diese zu kategorisieren und entsprechend den gefundenen Kategorien zu bewerten. Dies wird konkreter am Beispiel des Online-Votings analysiert. Außerdem wird hierbei zwischen der Manipulation durch einzelne Personen oder Gruppen unterschieden. Unter dem Gesichtspunkt der Gruppenmanipulation wird das Kollektiv „Anonymous“ näher betrachtet und dessen Mittel der Beeinflussung analysiert.

1.3 Vorgehensweise

Um einen ersten Hinweis auf Manipulationsmethodiken zu erhalten, wird ein bereits manipuliertes Online-Voting betrachtet um rückwirkend festzustellen wodurch dessen Ergebnisse verfälscht wurden sowie ein eigenes Fallbeispiel durchgeführt.

Um die Zielstellung zu erreichen, wird folgend damit begonnen, Manipulationsmethodiken zu evaluieren.

2 Evaluation: Manipulation durch Einzelne

2.1 Analyse durchgeführter Votings

2.1.1 Bandvote “Sachsen rockt!” Mittweida 2011

Standardszenario:

Der Bandvote wurde vom 18.04.2011 bis 08.05.2011 veröffentlicht. Durch Aufruf der URL[3]: `http://www.global.hs-mittweida.de/~cf/wordpress/?page_id=590` gelangte man direkt zur Bandabstimmung. Dort konnte zwischen den fünf Wahlmöglichkeiten eine favorisierte Band angeklickt werden. Durch Bestätigen auf „abstimmen“, erhielt dieser Vorschlag eine Stimme. Dies wurde dem Befragten ersichtlich durch die Inkrementierung der Stimmen des ausgewählten Vorschlages, textuell in Form von Prozenten und visuell in Form eines Balken. Die Teilnahme am Voting war ohne eine Anmeldung möglich, die einzige Sicherheitsmaßnahme war die Internet Protocol Adress-Filterung.[4]

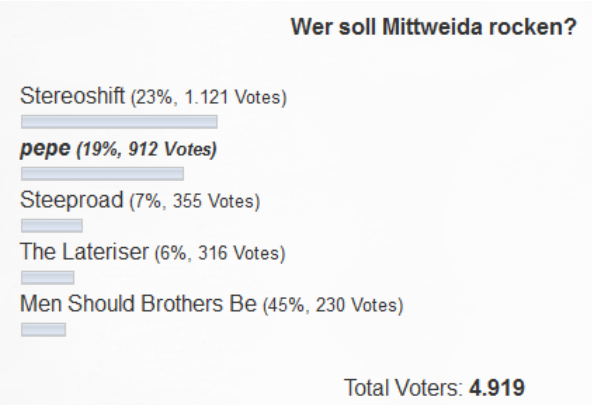


Abbildung 2: Abstimmung zum Bandvote “Sachsen rockt!” in Mittweida 2011[5]

[3] URL: Uniform Resource Locator, bezeichnet die eindeutige Adressierung einer Domain im Internet.

[4] Internet Protocol Adress-Filterung: Speicherung der bereits verwendeten IP-Adresse, um die Stimmabgabe eines Benutzers für dieses Voting einmalig zu halten.

[5] http://www.global.hs-mittweida.de/~cf/wordpress/, 02.05.12

Manipuliertes Szenario:

Die anonyme Stimmabgabe, folglich die Stimmabgabe per IP-Adresse kann manipuliert werden. Folgende drei Möglichkeiten werden beleuchtet:

- Zurücksetzen des Routers

  Ein Teilnehmer des Online-Votings kann durch Zurücksetzen des Routers eine neue IP-Adress-Vergabe erzwingen. Der Router ist dafür zuständig die Daten aus dem eigenen Netz weiterzuleiten (routen) bis in das Zielnetz. Als Adressat für das eigene Netz gilt die IP-Adresse. Durch Zurücksetzen des Routers und der damit verbundenen Trennung des eigenen Netzes vom Internet, wird beim Internetanbieter des Netzbesitzers eine neue IP-Adresse angefordert. Diese ermöglicht ein erneutes Abstimmen desselben Teilnehmers. Dieses manuelle Vorgehen kann durch den Einsatz von einfachen Skripten sowie durch den verteilten Einsatz dieser Skripte auf mehreren Rechnern automatisiert werden.

- Einsatz eines Proxy-Servers

  Stellt man keine direkte Verbindung zum Ziel her, sondern nutzt einen Proxy-Server, welcher sich in einem anderen Adressbereich befinden muss, wird das eigene Datenpaket anonym gemacht, indem dieses durch die IP-Adresse des Proxy-Servers an das Ziel geroutet wird. Durch den Einsatz mehrerer Proxy-Server kann ein Teilnehmer mehrfach Stimmberechtigung erhalten, ebenso mit dem Zurücksetzen des Routers.

- Einsatz eines Virtual Private Network (VPN)

  Wird sich in eine bestehende VPN-Verbindung eingewählt, so erhält man nach außen die IP-Adresse aus dem Adressbereich des VPN und nicht des eigenen Netzes, insofern das eigene Netz nicht dasselbe Netz ist. Dadurch ist es ebenfalls möglich, dass ein Teilnehmer mehrfach abstimmen kann. Ein Nachteil aus Sicht der Manipulation ist die Authentifizierung am VPN. Damit ist der Teilnehmer im Netz bekannt und kann einfacher identifiziert werden, im Gegensatz zu den bereits genannten anonymen Methoden.

2.1.2 Fallbeispiel Teammeeting über Doodle[6]

Standardszenario:

Eine geschlossene Terminumfrage wird nur mit den Benutzern geteilt, die sich in einem jeweiligen Team befinden.

Durch Aufruf der URL: `http://www.doodle.com/5ypkegwmd8m23ykntable` wird man direkt auf die Website von Doodle und zur erstellten Umfrage weitergeleitet. Die URL wird durch den Ersteller der Umfrage an alle Interessenten verteilt. Damit kommt trotz nicht vorhandenen Login-Mechanismus eine geschlossene Benutzergruppe zustande. Auf dieser besteht die Möglichkeit zwischen 20 Terminen zu wählen. Nach Angabe seines Namens und der Bestätigung auf “Speichern”, werden die ausgewählten Termine für die anderen Benutzer sichtbar. Durch den Einsatz von farbigen Zellen, kann so in einem großen Team schnell und effizient ein Treffen organisiert werden. Nach Ablauf des Termines am 01.11.2011 wird die Umfrage vom Ersteller abgeschlossen und damit beendet.

Abbildung 3: Übersicht der Doodleumfrage[7]

[6]Doodle: Ein Dienst, der die Möglichkeit bietet, eine Terminumfrage im Internet durchzuführen.
[7]http://www.doodle.com/5ypkegwmd8m23ykntable, 11.05.12

Manipuliertes Szenario:

Die Umfrage über Doodle kann leicht manipuliert werden, indem ein Benutzer angeklickt wird, welcher bereits an der Umfrage teilgenommen hat. Nun hat man die Möglichkeit seinen Eintrag zu bearbeiten oder diesen sogar komplett aus der Umfrage zu entfernen. Es ist also ohne Anmeldung oder andere Authentifizierung möglich diese Umfrage gezielt zu beeinflussen, unter der Voraussetzung, dass dem Angreifer die URL bekannt ist. Innerhalb der Benutzergruppe kann nicht nachvollzogen werden, wer welche Einträge beeinflusst hat. Es ist nicht notwendig einen eigenen Benutzernamen anzulegen.

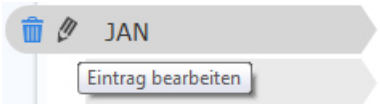


Abbildung 4: Bearbeitungsansicht innerhalb der Umfrage[8]

Durch diese Analysen ist ersichtlich, dass ein Online-Voting viele Möglichkeiten bietet das Resultat zu manipulieren. Folgend wird auf diesen Erkenntnissen aufgebaut und weitere Methodiken zur Verdeutlichung der Manipulationsmöglichkeiten bei Online-Votings beleuchtet sowie entsprechende Gegenmaßnahmen aufgezeigt.

2.2 Manipulationsmöglichkeiten und Gegenmaßnahmen

Die beiden vorangegangenen Fallbeispiele unterscheiden sich in ihrer Art der Manipulation. Zum einen Internet Protocol Adress-Filterung zum anderen als Manipulation geschlossener Benutzergruppen. Sie stellen nur ein Beispiel aus der Vielzahl an Möglichkeiten dieser Methodiken dar. Um dem Thema der vorliegenden Arbeit zu entsprechen, werden diese gezeigten Möglichkeiten nicht an weiteren Fallbeispielen vertieft, sondern weitere Methodiken in der Breite analysiert. Es wurden vier Manipulationsarten gewählt, welche sich grundlegend in ihrem Manipulationspotential unterschieden. In diesem Abschnitt wurde der Versuch unternommen, die verschiedenen Manipulationsmöglichkeiten klar voneinander abzugrenzen, um eine bessere Struktur zu schaffen. In der Realität lassen sich auf ein Online-Voting jedoch mehrere Manipulationen anwenden.

[8] http://www.doodle.com/5ypkegwmd8m23ykntable, 11.05.12

2.2.1 Cookies

Standardszenario:

Bestätigt der Benutzer seine Abstimmung des Online-Votings, wird bei dieser Variante eine Datei (Cookie) auf dem Rechner des Benutzers angelegt. Diese beinhaltet Datensätze, die den Rechner identifizieren und hindern somit ein erneutes Abstimmen[9]. Sollten Cookies für den Online-Vote benötigt werden, wird der User darauf hingewiesen.

Manipuliertes Szenario:

- Cookie löschen

  Das Löschen der Cookies kann über die Interneteinstellungen des Webbrowsers[10] geschehen. Alle gespeicherten Informationen über den Benutzer auf dieser Seite werden gelöscht. Damit wird der Benutzer wieder anonymisiert und als neuer Teilnehmer des Votings erkannt und kann erneut abstimmen.

- Verwendung eines anderen Webbrowsers

  Da der Cookie immer im jeweiligen Ordner des verwendeten Webbrowsers gespeichert wird, ist es möglich verschiedene Webbrowser zu benutzen und somit mehrfach abzustimmen.

Gegenmaßnahmen:

Basiert ein Online-Voting lediglich auf Cookie-Sicherheit, so ist dieses Voting sehr anfällig für Manipulation, da diese auf Seiten der Anwender im eigenen Webbrowser geschieht. Das Löschen von Cookies ist den meisten Benutzern bekannt sowie eine Vielzahl von Webbrowsern auf Anwenderrechnern existent.

[9] Vgl. Christl, 2008: 7

[10] Webbrowser: Ein grafisches Benutzerprogramm zum Darstellen von Websites im Internet.

2.2.2 E-Mail

Standardszenario:

Es existieren Online-Votings, welche die Bekanntgabe der eigenen E-Mailadresse voraussetzen um erfolgreich abzustimmen. Damit soll der Benutzer im Online-Voting identifiziert werden. Wurde einmal unter einer bestimmten E-Mailadresse abgestimmt, so kann keine erneute Teilnahme mit derselben E-Mailadresse erfolgen[11]. Die E-Mailadressen werden mit der zugehörigen Datenbank des Online-Votings auf Eindeutigkeit verglichen. Damit werden bereits eingetragene E-Mailadressen von Voting ausgeschlossen.

Manipuliertes Szenario:

Um mehrfach teilnehmen zu können, ist es möglich weitere E-Mailadressen bei bekannten Webhostern, wie zum Beispiel: Freenet, Web, Gmx, Googlemail anzulegen. Ein Benutzer besitzt eine E-Mailadresse bei Web und Googlemail und nutzt beide, um als Einzelperson doppelt abzustimmen. Der Aufwand zum Anlegen einer neuen E-Mailadresse, kann mitunter sehr zeitaufwendig sein, da komplette Anmeldeformulare ausgefüllt werden müssen. Eine Alternative zu diesem Verfahren bieten Trashmails. Anbieter von Trashmaildiensten stellen sofort neue E-Mailadressen ohne Anmeldung zur Verfügung, durch Aufrufen des Services. Auf `www.10minutemail.com` wird sofort eine E-Mailadresse generiert, die zehn Minuten existiert und bei Bedarf um weitere zehn Minuten verlängert werden kann. Dieser Service verkürzt den Manipulationsprozess enorm.

Gegenmaßnahmen:

Herkömmliche E-Mailadressen können durch geeignete Filtermechanismen zuverlässig von einer Mehrfachteilnahme ausgeschlossen werden. Weit verbreitete Trashmailhoster wie zum Beispiel: `www.trashmail.de` oder `www.trash-mail.com` können durch weitere Filter ausgeschlossen werden. Der spezielle Algorithmus zur Generierung der E-Mailadressen, wie auf der URL `www.10minutemail.com` erschwert die Filterung durch die zufällige Aneinanderreihung von Zeichen sehr.

[11] Vgl. Christl, 2008: 126

2.2.3 CAPTCHA

Abbildung 5: CAPTCHA-Abfragefenster[12]

Standardszenario:

"Der Begriff CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) [...] bezeichnet Verfahren, mit denen automatisch festgestellt werden kann, ob es sich bei einem Gegenüber um einen Menschen oder eben um eine Maschine handelt. Eingesetzt werden diese Techniken heute vor allem dazu, um automatisierten Programmen, so genannten Bots, den Zugang zu verschiedenen Internetdiensten, wie etwa der Registrierung von kostenlosen E-Mail-Accounts oder Benutzerkonten auf Websites, zu verwehren. [...] So muss der Benutzer etwa eine Buchstaben- oder Zahlenfolge abtippen, die vorher mit einem Bildfilter so verzerrt wurde, dass sie von einer Software nicht entziffert werden kann." [13]

Das heißt, eine erfolgreiche Teilnahme bedingt die Eingabe eines Zeichencodes.

Manipuliertes Szenario:

Diese Manipulation basiert auf der vollautomatischen Erkennung und Eingabe des CAPTCHA-Codes durch den Computer. Sind die abgebildeten Zeichen, der sogenannte CAPTCHA-Code nur minimal entfremdet von den Originalzeichen, so kann mittels des OCR (Optical Character Recognition) die Zeichenfolge ausgelesen werden. Der Algorithmus verläuft dreistufig, indem er erst die Seiten erkennt, danach Muster auf den Seiten und anschließend die erkannten Muster in ein für Menschen lesbares Ausgabeformat überführt[14]. Diese ausgelesene Zeichenfolge kann nun automatisch vom Computer in das vorgegebene Feld eingegeben und somit erfolgreich vollautomatisch am Online-Voting teilgenommen werden.

[12] http://www.1stwebdesigner.com/freebies/captcha-solutions-kill-spam/, 01.07.12
[13] Computerworld, 2007: 40
[14] Vgl. Ward 2011, http://rwservices.no-ip.info:81/pens/biblio90.html, 03.05.12

Gegenmaßnahmen:

Um den OCR-Algorithmus zu umgehen, kann der CAPTCHA-Code so weit entfremdet werden, dass der Computer die Zeichenfolge nicht mehr lesen kann. Im Umkehrschluss bedeutet dies, dass auch für den regulären Teilnehmer (Mensch) das Lesen der Zeichen erschwert wird, bis hin zur völligen Unkenntlichkeit. Um trotz dessen nicht auf diese entfremdete Form des CAPTCHA-Codes zu verzichten und die Sicherheit des Online-Votings zu erhöhen, können vom Benutzer weitere CAPTCHA-Codes angefordert werden.

2.2.4 Social Engineering

Standardszenario:

Durch Social Engineering ist es möglich neben den technischen Mitteln der Online-Votingmanipulation auch menschliche Schwachstellen zu finden und zu beeinflussen, um zum gewünschten Ergebnis, der Manipulation, zu gelangen. "Social Engineering kostet nichts und überwindet alle technologischen Barrieren, weil es geschickt das Vertrauen und die Neugier der Menschen ausnutzt."[15] So der Ex-Hacker Kevin Mitnick, der ein Spezialist auf dem Gebiet des Social Engineering ist, was sinngemäß als soziale Manipulation bezeichnet werden kann. Diese Manipulation kann also auch angewandt werden, um beispielsweise einen Administratorzugang zu einem Online-Voting zu erhalten und dieses mit den Zugriffsrechten zu beeinflussen.

Manipuliertes Szenario:

Unter dem Sammelbegriff Social Engineering verbirgt sich eine Vielzahl von Manipulationsmöglichkeiten. Eine besser Struktur dieser Manipulation ist durch folgende Kategorisierung gegeben:[16]

- Human Based Social Engineering (HBSE) - Eine Manipulation von Mensch zu Mensch, durch Rhetorik, soziales Einfühlungsvermögen, Autorität, Selbstsicherheit, Kreativität und kommunikatives Geschick.

[15] Lochmaier 2007, http://www.zdnet.de/magazin/39152145/risikofaktor-mensch-die-kunst-des-social-engineering.htm, 01.07.12
[16] Lipski, 2009: 7 f.

- Computer Based Social Engineering (CBSE) - Beschaffung von Informationen mit Hilfe von technischen Hilfsmitteln, bspw. Phishing.

- Reverse Social Engineering (RSE) - Durch intensive Vorbereitung auf Seiten des Social Engineers meldet sich das Manipulationsopfer selbst bei diesem. Zum Beispiel wurde im Vorfeld der PC des Opfers manipuliert, damit dieser einen Techniker anruft. Die Telefonnummer des Technikers wurde mit der des Social Engineers ersetzt.

Alle Vorgehensweisen haben das Ziel an Passwörter oder private Daten zu gelangen. Im Vorfeld erkundigt sich der Social Engineer über Informationen seines Manipulationsopfers, wie berufliche Daten, um einen möglichst seriösen Eindruck zu vermitteln. Beim gezielten Manipulieren von Online-Votings können so User- oder Admin-Accounts generiert werden, um so einzugreifen. Diese Form der Manipulation ist sehr vielversprechend, da das schwächste Glied in der Kette meistens der Mensch darstellt, egal wie viel Geld für hochmoderne Sicherheitstechnik ausgegeben wird. Versagt der Mensch, versagt das System. Der Sicherheitsberater Bruce Schneider beschreibt das Problem so: „Sicherheit ist kein Produkt, sondern ein Prozess. Darüber hinaus ist Sicherheit keine technologische Angelegenheit, sondern ein menschliches und ein Management-Problem.“[17] Es muss also nicht daran liegen, dass eine Person naiv ist und deshalb auf einen Social-Engineer reinfällt, viel mehr sind die Meisten nicht vertraut mit aktuellen Sicherheitspraktiken.

Gegenmaßnahmen:

Es gibt kein technisches Mittel um gegen das Social Engineering vorzugehen. Vielmehr muss der Mensch als Sicherheitslücke richtig geschult werden, um die Risiken dieser Manipulation zu unterbinden. Dieser fühlt sich in der heutigen Zeit so sicher hinter Firewalls, dass er leichtsinnig wird und damit dem Social Engineer in die Falle läuft. Außerdem ist es von Vorteil, wenn jeder Mitarbeiter nur Zugriff auf die für seine Aufgaben relevanten Daten und Informationen erhält.

Maßnahmen zur Erkennung von Social Engineering:

„- sensible Daten klassifizieren sowie Prozeduren und Prozesse abstimmen
- die Mitarbeiter konsequent instruieren und weiterbilden
- das Bewusstsein in praktischen Trainings erhöhen
- Varianten des Social Engineerings in akute Maßnahmenpläne integrieren.“[18]

[17] Mitnick/Simon/Dubau, 2006: 20

[18] Lochmaier 2007, http://www.zdnet.de/magazin/39152145/risikofaktor-mensch-die-kunst-des-social-engineering.htm, 01.07.12

2.3 Resümee: Manipulationsarten durch Einzelne

Um die Methodiken bzw. Manipulationsmöglichkeiten besser einzuordnen, werden sie in verschiedene Arten eingeteilt sowie nach Kriterien bewertet. Nachfolgende Tabelle bezieht sich lediglich auf die Fallbeispiele sowie auf die in dem vorhergehenden Abschnitt behandelten Methodiken und bietet daher einen ersten Überblick über weit verbreitete Manipulationen in Online-Votings. Es existieren noch unzählige andere Manipulationsarten, die sich jedoch in ihrer Ausprägung zu großen Teilen in die gefundenen Kategorien eingliedern lassen. Manipulation an der Vertraulichkeit meint das Vortäuschen falscher Identitäten in geschlossenen Benutzergruppen.

Die betrachtete Benutzergruppe ist der reguläre Benutzer.[19]

Manipulationsart	Zugang	Vollautomatisch	Zuverlässigkeit
IP	schwer	ja	ja
Vertraulichkeit	normal	ja	ja
Cookie	einfach	ja	nein
E-Mail	normal	ja	nein
CAPTCHA	schwer	ja	nein
Social Engineering	schwer	nein	ja

Tabelle 1: Evaluierte Manipulationsarten durch Einzelne

Legende:

- Zugang:
  - einfach...Für alle Benutzer ist diese Manipulationsart auszuführen
  - normal...Für die meisten Benutzer ist diese Manipulationsart auszuführen
  - schwer...Für die wenigsten Benutzer ist diese Manipulationsart auszuführen
- Vollautomatisch
  - ja...Vollständig durch den Computer automatisierbar
  - nein...Teilweise durch den Computer automatisierbar

[19] Der reguläre Benutzer definiert sich durch alltägliche Kenntnisse im Umgang mit Computer und Internet.

- Zuverlässigkeit
  - ja...Weitestgehend erfolgreiche Manipulation, ohne von Gegenmaßnahmen gestoppt zu werden
  - nein...Weniger erfolgreiche Manipulation, ohne von Gegenmaßnahmen gestoppt zu werden

Im nächsten Abschnitt werden Manipulationsarten durch Gruppen evaluiert.

3 Evaluation: Manipulation durch Gruppen

3.1 Einführung in das Thema am Beispiel von Anonymous

Bevor begonnen wird die Manipulationsmethoden von Anonymous zu evaluieren, ist es wichtig zu wissen, was diese Gruppe eigentlich repräsentiert. „Anonymous ist keine Gruppe, bei der man Mitglied werden kann, sondern eine – manchmal ziemlich vage – Idee, der man sich zugehörig fühlt. In Foren und Chats nehmen die Anhänger Kontakt zu Gleichgesinnten auf und schließen sich spontan einer Operation an. Oder sie rufen gleich selbst eine Aktion aus. Anonymous-Anhänger wehren sich vehement gegen die Bezeichnungen »Gruppe« und »Mitglied«. [. . .] Für diese Form der losen Verabredung und gemeinsamer Werte verwenden die Anonymous-Aktivisten den Begriff »Kollektiv«.“[20] Jeder Internetnutzer kann sich also diesem Kollektiv anschließen und mit ihnen agieren. Es gibt innerhalb des Zusammenschlusses keine Instanzen, sondern nur Grundregeln, welche eingehalten werden sollen. Darin besteht auch die Stärke von Anonymous, die unzähligen Sympathisanten des Kollektivs. Anfangs belächelt, wurden sie schnell zu ernstzunehmenden Aktivisten, die für ihre Überzeugung „Freiheit im Internet“ kämpfen.

3.2 Mittel der Manipulation

Nachfolgend werden Programme, Fachbegriffe oder Vorgehensweisen von Anonymous dargestellt und erklärt, welche bei der Beeinflussung von Online-Votings eingesetzt werden. In den folgenden Kapiteln werden diese anhand von praktischen Beispielen verdeutlicht.

IRC

„Dies ist ein Mehrbenutzer – Kommunikationssystem, auf dem sich Leute auf sogenannten „Channels“ (Gesprächskanäle) in Gruppen oder einzeln unterhalten können. Benutzer des Systems sind durch einen „Nickname“ (Spitzname / Pseudonym) gekennzeichnet.“[21] Zudem bietet IRC (Internet Relay Chat) die Möglichkeit private Chaträume einzurichten, in die man nur auf Einladung hineinkommt. Ohne

[20] Reissmann/Stöcker/Lischka, 2012: 5 f.
[21] Schmitt, 2010: 3

diese Möglichkeit der Absprache wäre es für Anonymous nicht möglich Angriffe zu planen und diese zeitgleich auszuführen.

Loic

Da nicht davon ausgegangen werden kann, dass alle Anhänger von Anonymous umfangreiche Kenntnisse in Programmierung haben können, wird ein simples Tool namens Loic (Low orbit ion cannon) eingesetzt. Diese Anwendung bietet jedem die Chance bei den Angriffen und Manipulationen teilhaben zu können. „Ursprünglich wurde das Programm 2006 entwickelt, um zu Testzwecken massenhaft Datenpakete zu verschicken.“[22] Im Kapitel 3.2.2 wird anhand eines Beispiels auf die Funktionsweise von Loic eingegangen.

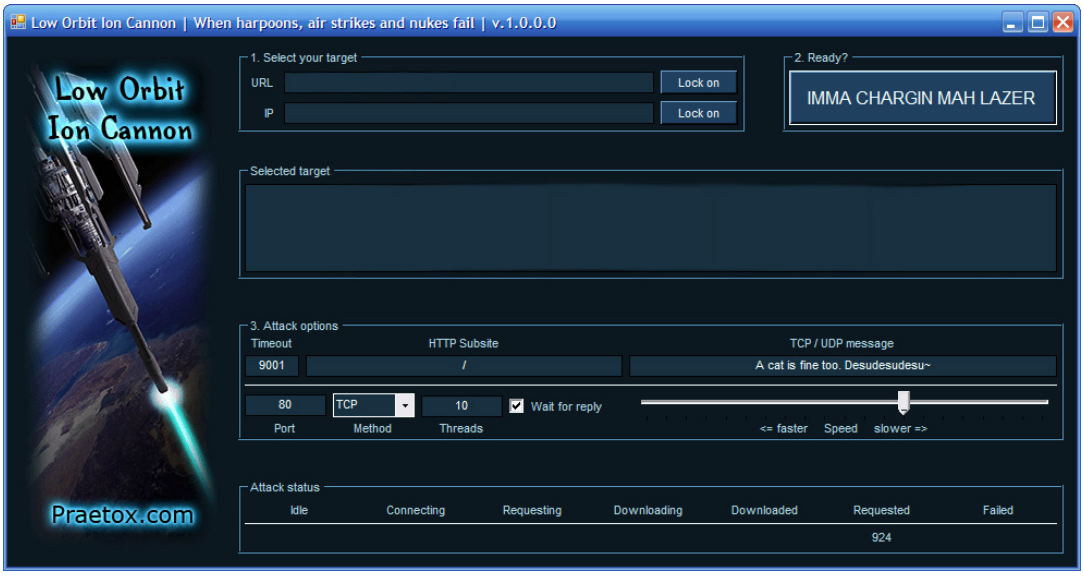


Abbildung 6: Anwendung “Loic”[23]

DoS/DDoS-Attacken

„DoS-Attacken sind Angriffe, welche zum Ziel haben, den betroffenen Host lahmzulegen. Ein Rechner kann auf verschiedene Arten unerreichbar gemacht werden. Man bombardiert ihn mit Paketen, die seine Ressourcen völlig ausschöpfen und ihn sogar zum Absturz bringen können. Die Ressourcen eines Rechners sind die Prozessorleistung, Arbeitsspeicher oder die Bandbreite der Netzwerkanbindung. Bei einem solchen Angriff ist der Host so stark ausgelastet, dass es

[22] Reissmann/Stöcker/Lischka, 2012: 39
[23] http://www.planetshaker.de/wp-content/uploads/2010/12/Loic1.jpg, 01.07.12

ihm nicht mehr möglich ist seinen eigentlichen Aufgaben nachzugehen. DDoS-Attacken sind DoS-Attacken, die von mehreren Standorten gleichzeitig ausgehen. Von DDoS spricht man ab ungefähr 50 beteiligten Angriffsrechnern.“[24] Von Anonymous selbst wird diese Attacke als friedliche Protestform im Internet bezeichnet, da hierbei ähnlich wie bei einer Sitzblockade, der Eingang für den Besitzer blockiert wird.

Social Media

Auf dem Videoportal YouTube[25] werden kurze Clips veröffentlicht um ein neues Projekt anzukündigen. Dadurch bekommen sie Aufmerksamkeit und haben so die Möglichkeit neue Anhänger für einen Angriff zu gewinnen. Twitter[26] wird genutzt, um aktuelle Berichte über den Verlauf eines Projektes zu publizieren. Dieser Informationsfluss kann nur schwer gestoppt werden, da jeder Internetnutzer mit einem Link die benötigten Informationen schnell erhält. Blockiert ein Land die gesamte Website ist es ebenfalls über Proxy-Server möglich auf diese zu gelangen.

Botnetz

„Unter einem Botnet oder Zombienetz versteht man ein fernsteuerbares Netzwerk von Rechnern, das aus kommunizierenden Bots – autonomen Computerprogrammen für spezifische Aufgaben – besteht. Die Kontrolle wird durch Viren oder Trojaner erreicht, die die Rechner infizieren und Anweisungen ausführen.“[27] Der Einsatz eines Botnetzes wird im Kapitel 3.2.2 näher betrachtet.

Online-Community

Ohne die Hilfe einer großen Community können Kollektive wie Anonymous nicht existieren. Und ohne die Macht der Masse können keine Manipulationen im großen Rahmen durchgeführt werden. International ist die Online-Community auf `www.4chan.org` die Größte, wenn es um die Manipulation im Internet geht. Außerdem wird auf nationaler Ebene die deutsche Community von `www.readmore.de` näher beleuchtet.

[24] Studer, 2010: 110
[25] Ein Internet-Videoportal, zum Ansehen und Hochladen von Video-Clips.
[26] Eine Kombination aus kostenlosem Kurznachrichtendienst, Blog und E-Mail.
[27] Computerworld, 2007: 32

In den folgenden Abschnitten werden an konkreten Beispielen die Vorgehensweisen von Anonymous verdeutlicht.

3.2.1 Online-Community

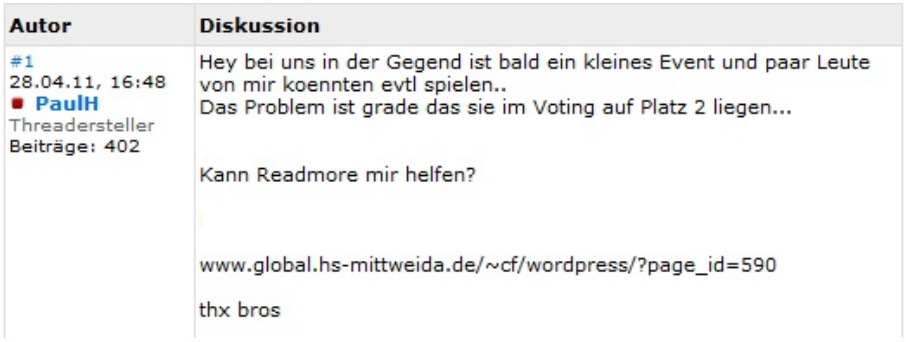
Allgemein

Die Online-Community wird auch als Web- oder Virtual-Community bezeichnet. Da bei dieser Form der Kommunikation das Internet verwendet wird, zeichnet sich diese besonders durch ihre Anonymität aus. „Jedem Teilnehmer ist es selbst überlassen, ob er seinen echten Namen und seine Identität preisgibt oder anonym bleibt. Durch diese Anonymität und die fehlende reale Gegenüberstellung der Mitglieder wird die Überschreitung von sozialen Grenzen erleichtert, man kann auch leichter andere Rollen ausprobieren. [. . .] Die Online-Community kann als der zentrale Plattformtyp des Web 2.0 betrachtet werden, da dort viele typische Elemente des Web 2.0, wie z.B. Foren, integrierte Blogs und/oder RSS-Feeds[28], vertreten sind.“[29]

Ohne eine entsprechende Plattform können keine Online-Communities entstehen. Diese Plattform stellt das Online-Forum für die User dar. „Online-Foren bieten die Möglichkeit, Diskussionsbeiträge (Postings) zu hinterlassen, die gelesen und direkt beantwortet werden können. [. . .] Die Folge aus Initialbeitrag und Antworten zu einem Thema (Topic) wird als Faden (Thread) bezeichnet. Zumindest für die Betreiber eines Forums besteht also die Möglichkeit, Kontakt zu Verfassern einzelner Beiträge aufzunehmen. Foren gehören zum engeren Kern der Online-Communities, da als Voraussetzung zum Verfassen eigener Beiträge eine Registrierung nötig ist und damit eine sehr direkte Kommunikation zwischen Mitgliedern einer Forengruppe existiert.“[30] Jeder User kann also beispielsweise zu einer Aktion aufrufen, in der sich das gesamte Forum an einem Online-Voting beteiligen soll. Dazu muss er lediglich im Forum registriert sein um einen neuen Thread zu erstellen und in diesem Beitrag den Link vom Online-Votings veröffentlichen zu können. Durch die Vielzahl der Nutzer wird nun das Ergebnis in die Richtung manipuliert, welche die Community möchte.

Wie im Kapitel 2.1.1 beschrieben, wurde dieses Manipulationsverfahren beim Campus Festival 2011 in Mittweida eingesetzt. Dabei wurde auf der Website von “Readmore” ein Thread mit dem Namen „Bandvoting, need Help!“ eröffnet.

[28] Eine Art Nachrichten-Ticker im Internet.
[29] Finster, 2011: 19
[30] Weiss, 2008: 23



Autor	Diskussion
#1 28.04.11, 16:48 PaulH Threadersteller Beiträge: 402	Hey bei uns in der Gegend ist bald ein kleines Event und paar Leute von mir koennten evtl spielen.. Das Problem ist grade das sie im Voting auf Platz 2 liegen... Kann Readmore mir helfen? www.global.hs-mittweida.de/~cf/wordpress/?page_id=590 thx bros

Abbildung 7: Eintrag im Forum auf “Readmore”[31]

Nach diesem Aufruf dauerte es nicht lange und die gewünschte Band erlangte den ersten Platz im Online-Voting. Das Forum von „Readmore“ existiert seit dem Jahr 2005 und hat seit der Gründung eine große Community aufgebaut. Da es sich um ein eSport-Forum handelt, also den Bereich Computer- und Internetspiele abdeckt, sind hier viele User angemeldet, welche viel Allgemeinwissen von Computern und dem Internet haben und auch gern bei der Manipulation von Votings behilflich sind.

Online-Community: Anonymous

Am besten lässt sich die Macht der Online-Community von Anonymous am Beispiel vom TIME-Voting demonstrieren. Die TIME ist ein wöchentlich erscheinendes amerikanisches Nachrichtenmagazin und stellt jedes Jahr eine Tabelle mit den 100 einflussreichsten Persönlichkeiten auf. Vorab konnte im Internet, als eine Art PR-Kampagne, über die Zusammensetzung dieser Tabelle abgestimmt werden. Neben berühmten oder politischen Persönlichkeiten, nahmen die Redakteure des Magazins ebenfalls einen gewissen Christopher „moot“ Poole mit in die Liste auf. Dieser „moot“ ist der Gründer der Website “4chan”, welche über eine riesige Online-Community verfügt. „4chan-Gründer Christopher ’moot’ Poole berichtet selbst von 10 Millionen Unique Users im Monat – das hieße, dass jeden Monat 10 Millionen mal von verschiedenen Computern oder Webbrowsern aus auf das Forum zugegriffen wird.“[32]

Nutzer dieses Forums sind größtenteils die sogenannten Freaks und Nerds, welche überdurchschnittlich viel Zeit im Internet verbringen und gut mit allen aktuellen diesbezüglichen Gegebenheiten vertraut sind. Nachdem bekannt wurde, dass ihr Foren-Gründer „moot“ mit auf der Liste ist, entschieden sich einige User

[31] http://www.readmore.de/index.php?cont=forum/thread\&threadid=89303\&page=1, 01.07.12
[32] Reissmann/Stöcker/Lischka, 2012: 71

für ihn zu voten. Um besser organisiert an dieses Online-Voting heran zu gehen, gründeten sie ein Kollektiv mit dem Namen Anonymous. Da dieses Voting nicht mit normalen Mitteln gewonnen werden konnte, wurde dies mit sogenannten Autovotern realisiert.

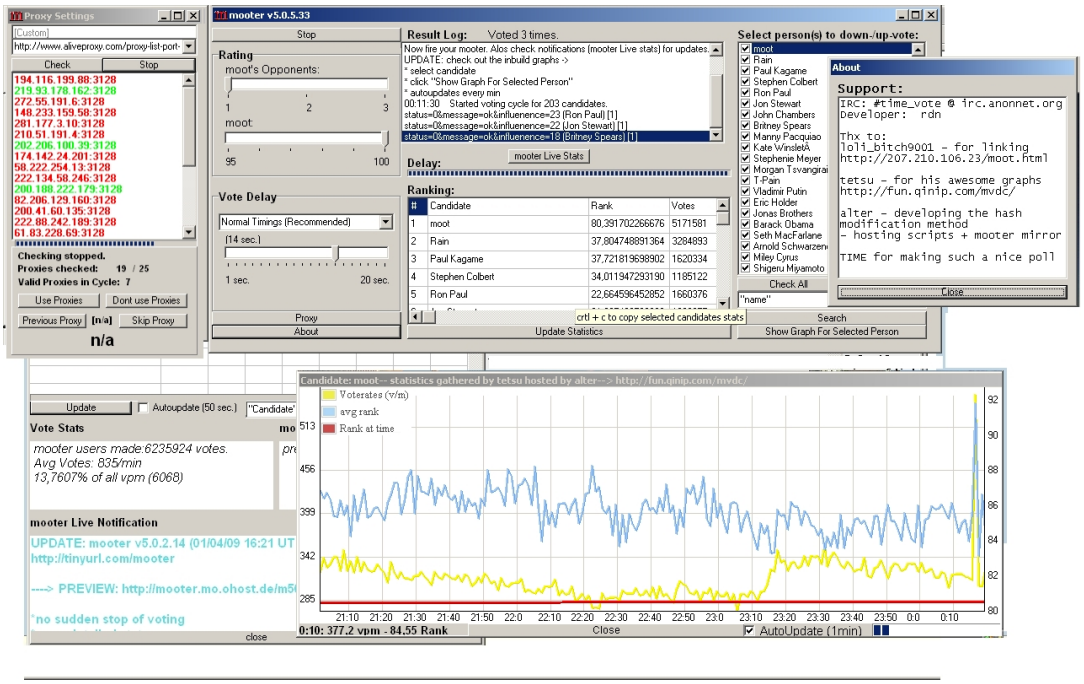


Abbildung 8: Anwendung Autovoter “Mooter”[33]

Diese Autovoter stimmen kontinuierlich für eine oder mehrere Optionen innerhalb des Online-Votes ab. Da dieses Voting der TIME mit keinen Sicherheitsmechanismen ausgestattet war, konnten die Anwendungen ungehindert arbeiten. Dabei konnten diese Programme bis zu 300 Votes in der Minute von einer einzigen IP-Adresse abgeben. Die nachfolgende Grafik verdeutlicht das Ausmaß der Manipulation.

[33]http://musicmachinery.com/2009/04/27/moot-wins-time-inc-loses/, 01.07.12

Rank	Name	Avg. Rating	Total Votes
1	moot	90	16,794,368
2	Anwar Ibrahim	47	2,316,378
3	Rick Warren	45	1,902,542
4	Baitullah Mehsud	45	1,902,162
5	Larry Brilliant	44	2,005,310
6	Eric Holder	43	1,808,663
7	Carlos Slim	41	1,852,506
8	Angela Merkel	41	1,634,488
9	Kobe Bryant	39	1,977,676
10	Evo Morales	39	1,477,789
11	Alexander Lebedev	38	824,586
12	Lil' Wayne	37	939,993
13	Sheikh Ahmed bin Zayed Al Nahyan	36	839,034
14	Odell Barnes	35	916,836
15	Tina Fey	33	897,045
16	Hu Jintao	32	928,400

Abbildung 9: Manipuliertes TIME-Voting[34]

Gegenmaßnahmen: Anonymous

Nachdem dies auch den Administratoren des Online-Votings auffiel, setzten sie CAPTCHA-Authentifizierungen ein, um die „Autovoter“ zu unterbinden. Anonymous musste sich somit einer anderen Art der Manipulation bedienen. Durch die Masse an Unterstützern des Kollektivs, wurden die CAPTCHA-Codes einfach von Hand eingegeben. Dagegen konnten die Betreiber des Online-Votings nichts ausrichten und mussten zusehen, wie ihre PR-Kampagne von hunderten Internetusern manipuliert wurde.

[34] http://musicmachinery.com/2009/04/15/inside-the-precision-hack/, 01.07.12

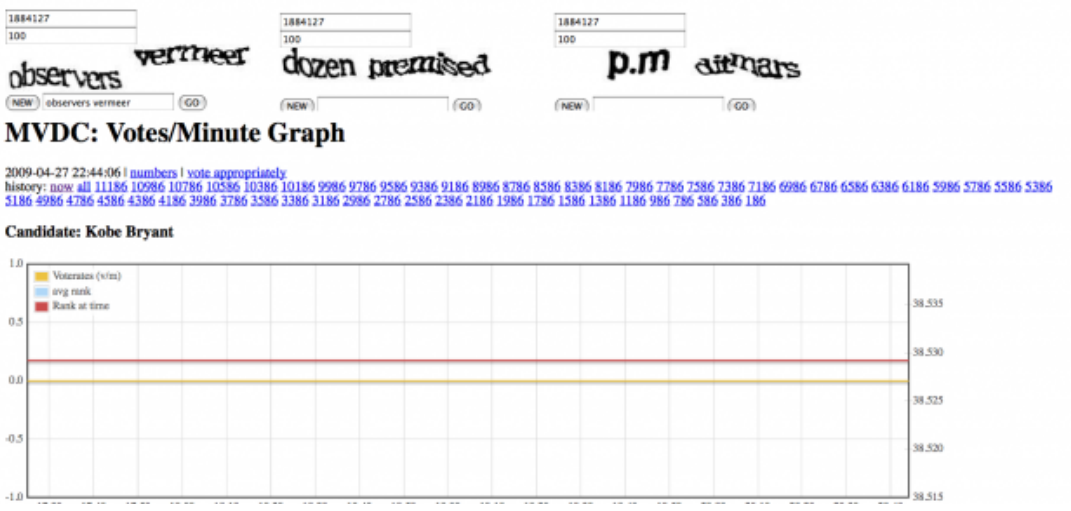


Abbildung 10: Eingabe der CAPTCHA-Codes[35]

Gegenmaßnahmen: Allgemein

Ein wirkungsvolles Mittel gegen eine große Gruppe von manipulierenden Votern gibt es nicht. Es ist jedoch möglich, eine Abstimmung zu privatisieren. Dies kann mit der Voraussetzung verknüpft sein, dass nur über das Konto eines Social Networks (beispielsweise Facebook) abgestimmt werden kann. Allerdings kann dies auch das Ergebnis negativ beeinflussen, da ehrliche Voter ebenfalls nicht ihre Identität via Facebook preisgeben möchten.

Um gezielt gegen eine Gruppe vorzugehen, ist es möglich Stimmabgaben zu löschen, um somit die Motivation derjenigen negativ zu beeinflussen die absichtlich manipulieren. Somit wird allerdings auch wieder aktiv in die Abstimmung eingegriffen und diese verliert somit den repräsentativen Charakter.

Auswirkungen: Anonymous

Das Magazin TIME trägt durch diese Manipulation keinen großen Schaden, da das Voting nur für Marketing Zwecke und Öffentlichkeitsarbeit gedacht war. Dieses Beispiel zeigt allerdings eindeutig, dass diese Abstimmungen im Internet keinerlei journalistische Relevanz haben. Nimmt sich eine Gruppe vor ein Online-Voting zu manipulieren, dann kann in den wenigsten Fällen dagegen vorgegangen werden. Die Betreiber und Administratoren müssen zusehen, wie ihre Ergebnisse verfälscht werden.

[35] http://musicmachinery.com/2009/04/15/inside-the-precision-hack/, 01.07.12

3.2.2 Botnetz

Allgemein

Zur Entstehung eines Zombienetzwerkes reicht ein infizierter Rechner aus. Dies kann mittels eines Trojaners geschehen, welcher unwissentlich über das Internet heruntergeladen wird. Anschließend setzt sich dieser im System des Betroffenen fest, ohne das der Benutzer etwas bemerkt. Wie geschickt die Entwickler der Schadsoftware dabei vorgehen, zeigt sich an einem aktuellen Beispiel aus dem Jahr 2012. Der Trojaner mit der Bezeichnung „Flame“ gelangte auf tausende Rechner, indem er sich als Windows-Update samt gefälschten Microsoft-Zertifikat ausgab und somit bedenkenlos auf die Festplatten der Endnutzer gelangte[36].

„Eine fundamentale Aufgabe eines jeden Zombies besteht darin, weitere Clients zu infizieren, damit das Botnetz möglichst schnell expandiert. Eine Möglichkeit dies zu bewerkstelligen besteht darin, nach potentiellen Opfern zu scannen.“[37] Besitzt eine Person die Kontrolle über eine große Anzahl an Zombierechnern, kann er diese nutzen, um DDoS-Attacken zu starten oder auch um mit vielen Rechnern an Online-Votings teilzunehmen und diese damit zu manipulieren.

Botnetz: Anonymous

Im Fall Anonymous haben Botnetzwerke eine besondere Bedeutung, da sie bewusst für Anonymous zur Verfügung gestellt werden. Jeder Sympathisant von Anonymous oder einer von ihnen gestarteten Aktion trägt zum Erfolg der Manipulation bei. „Eine klare Trennung zwischen Tätern und Zuschauern gibt es dabei nicht: Jeder kann mitmachen, es dauert nur Minuten, denn Hacker-Qualitäten braucht man nicht. Selbst der, der die »Ionenkanone« Loic nicht einsetzt, sondern nur während einer Attacke nachschaut, ob eine Seite wirklich weg ist, trägt zur Überlastung der Seite bei. Der Einsatz der Software ist einfach: Einen Serienbrief mit Word zu erstellen ist schwieriger, als an einem Loic-Angriff teilzunehmen.“[38]

In dem bereits beschriebenen Programm Loic befindet sich eine Funktion namens „Hivemind“. „In diesem Modus wartet das Programm darauf, dass in einem bestimmten Chatkanal (IRC) ein Ziel bekannt gegeben wird, um automatisch loszuschlagen. Dazu muss der Besitzer nicht einmal in der Nähe sein, er kann seinen Rechner auch einfach laufen lassen.“[39] Je größer das Botnetz ist, umso größer ist die Datenmenge, welche beim DDoS-Angriff an den Zielserver

[36] Vgl. Eikenberg 2012, http://www.heise.de/security/meldung/Windows-Update-kompromittiert-1605393.html, 01.07.12
[37] Wagner, 2011: 27
[38] Reissmann/Stöcker/Lischka, 2012: 41
[39] Reissmann/Stöcker/Lischka, 2012: 40

übermittelt wird. Um dieses Vorgehen besser zu verdeutlichen wird ein Manipulationsbeispiel aus dem Jahr 2011 näher beleuchtet. Der Henkel-Konzern nutzte eine virale Werbekampagne um für ihr Spülmittel Pril zu werben. Dabei konnten Internetnutzer eigene Flaschenmotive designen und anschließend online zur Abstimmung stellen. Die Motive mit den meisten Stimmen sollten später produziert und vertrieben werden. Durch die Tatsache, dass es sich dabei wieder um ein großes Online-Votingverfahren handelte, dauerte es nicht lange, bis Anonymous darauf Aufmerksam wurde.

Abbildung 11: Aufruf “Operation Pril”[40]

Im Forum von “4chan”, in welchem Anonymousmitglieder aktiv sind, wird bewusst zur Manipulation des Votings aufgerufen. Es wird vermutet, dass andere Teilnehmer ebenfalls Bots einsetzten, um für ihre Designkonzepte zu stimmen. Das Motiv „PRIIIL“ von Anonymous wird in kürzester Zeit auf Platz 1 der Abstimmung gevotet. Damit ist den Betreibern der Kampagne klar, dass etwas nicht mit rechten Dingen zugeht[41].

Gegenmaßnahmen: Anonymous

Die Administratoren veröffentlichten eine Pressemitteilung bezüglich des Wahlbetrugs und löschten darauf eine große Menge an abgegeben Stimmen, die im

[40] http://www.24htrickster.net/wbb/small-talk/17760-operation-pril/, 10.07.12
[41] Vgl. Breithut 2011, http://www.spiegel.de/netzwelt/netzpolitik/soziale-netzwerke-pril-wettbewerb-endet-im-pr-debakel-a-763808.html, 11.07.12

Verdacht standen manipuliert worden zu sein. Da keine weiteren Sicherheitsmaßnahmen getroffen wurden, konnte die Manipulation am Voting fortgesetzt werden.

Gegenmaßnahmen: Allgemein

Um über Gegenmaßnahmen nachdenken zu können, sind vorerst Überlegungen zum Botnetzaufbau zu machen. Normale Botnetze werden in 2 Architekturen eingeteilt, die zentralisierte und dezentralisierte Topologie.

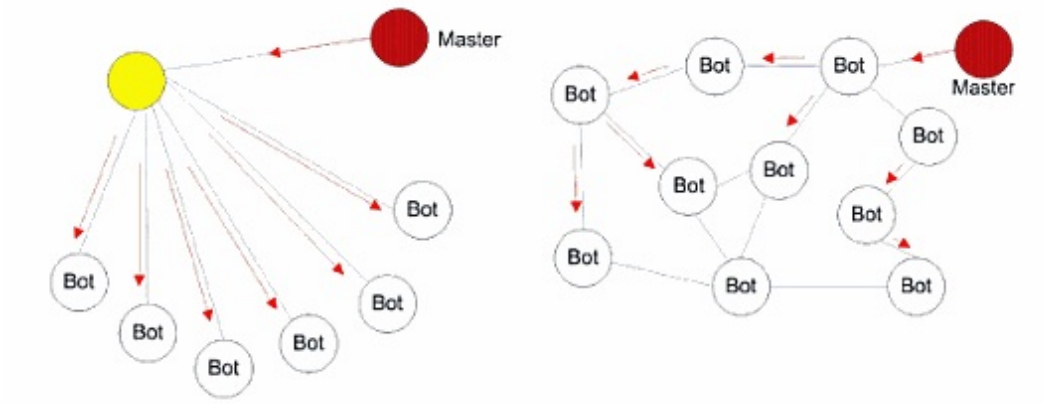


Abbildung 12: Zentrale und dezentrale Topologie[42]

„Ein zentrales Administrationssystem ist mit jedem Zombie-PC im Netzwerk verbunden. Neue Bots werden in eine Datenbank der Steuerungszentrale aufgenommen; zudem wird ihr Status beobachtet. Des weiteren erhalten sie vom Botnetzbetreiber Befehle. [. . .] Botnetze mit zentralisierter Topologie werden am meisten eingesetzt, da sie mit relativ wenig Aufwand aufzubauen sind und die Befehle schnell kommuniziert werden.“[43] Auf diese Weise agiert auch Anonymous bei ihren Angriffen. Es ist also theoretisch möglich die zentrale Stelle ausfindig zu machen und lahm zu legen, somit wäre das Botnetz stillgelegt.

Die dezentralisierte Topologie ist wenig bis gar nicht zu beeinflussen. „Bei diesem Netzwerktyp sind Bots mit einigen benachbarten Zombie-PCs verbunden, deren Adressen sie besitzen. Ankommende Befehle werden an diese Adressen weitergesendet. Der Botnetzverwalter sendet seine Befehle nur an einen beliebigen Zombie-PC und erreicht so alle Bots.“[44] Durch das Fehlen eines zentralen Rechners ist die Beseitigung dieses Netzwerkes kaum zu realisieren.

[42] Morawe, 2009: 15
[43] Morawe, 2009: 14
[44] Morawe, 2009: 15

Auswirkungen: Anonymous

Abbildung 13: Gewinner des Votings[45]

Nach Beendigung des Online-Votings stand das manipulierte Design auf dem ersten Platz. Durch das Löschen vieler Stimmen seitens Henkel waren ebenfalls unschuldige Teilnehmer des Online-Votings betroffen. Die Proteste über den Wahlbetrug und der damit entstandene Imageschaden für Henkel waren groß. Die Abstimmung und damit die Web 2.0 Kampagne waren gescheitert[46].

[45] http://robertlecker.wordpress.com/2011/05/18/die-causa-pril-und-andere-social-media-problemchen/, 01.07.12

[46] Vgl. Breithut 2011, http://www.spiegel.de/netzwelt/netzpolitik/soziale-netzwerke-pril-wettbewerb-endet-im-pr-debakel-a-763808.html, 11.07.12

3.3 Resümee: Manipulationsarten durch Gruppen

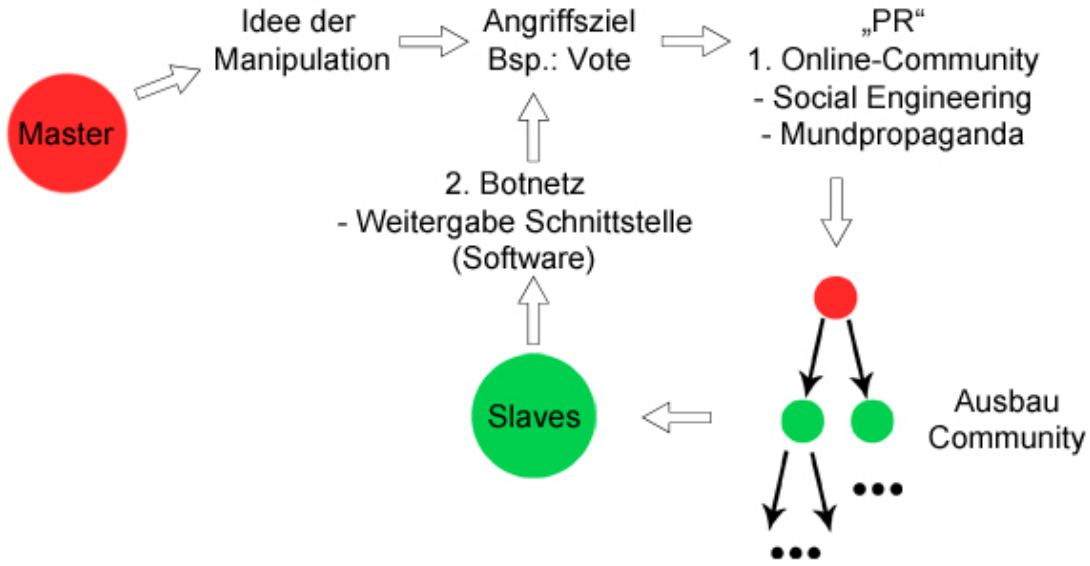


Abbildung 14: Zyklus Manipulation durch Gruppen[47]

Der Master[48] verfolgt die Idee ein Online-Voting zu manipulieren. Er verbreitet seine Idee und die Möglichkeiten als eine Form der Öffentlichkeitsarbeit in Foren. Durch die Teilnahme und Verbreitung der Forennutzer (Slaves[49]) expandiert die Gruppe in Form des Schneeballprinzips. Durch die Gewinnung neuer Gruppenmitglieder erweitern sich auch die Fähigkeiten auf unterschiedlichen Interessengebieten. Spezielle Software, welche eine umfassendere Manipulation ermöglicht, ist durch das steigende Know-How der Gruppe einfacher zu organisieren. Dieser Zyklus läuft kontinuierlich, bis das jeweilige Ziel erreicht wird.

Die Manipulationsmöglichkeiten durch Gruppen werden, wie bei der Evaluierung der einzelnen Personen, ebenfalls nach Kriterien bewertet. Die Einordnung erfolgt nach den Erkenntnissen, welche in den vorangegangen Kapiteln evaluiert wurden.

Die betrachtete Benutzergruppe ist wieder der reguläre Benutzer.

[47] Darstellung des Autors
[48] Befehlssender
[49] Befehlsempfänger

Manipulationsart	Arbeitsaufwand Master	Verbreitung	Zuverlässigkeit
Online-Community	einfach	einfach	ja
Botnetz	schwer	einfach	ja

Tabelle 2: Evaluierte Manipulationsarten durch Gruppen

Legende:

- Arbeitsaufwand Master
  - einfach...Der Masterkreis muss über wenig technische Kompetenzen verfügen
  - normal...Der Masterkreis muss über gute technische Kompetenzen verfügen
  - schwer...Der Masterkreis muss über hohe technische Kompetenzen verfügen
  - technische Kompetenzen: Softwareentwicklung, Computerarchitektur, verteilte Systeme...
- Verbreitung
  - einfach...Durch Vorarbeit des Masters enorm hohe Verbreitungsdichte
  - normal...Durch Vorarbeit des Masters gering Verbreitungsdichte
  - schwer...Durch Vorarbeit des Masters enorm geringe Verbreitungsdichte
  - Vorarbeit des Masters: Softwareschnittstelle / Angriffsziel zur Verfügung stellen
- Zuverlässigkeit
  - ja...Weitestgehend erfolgreiche Manipulation, ohne von Gegenmaßnahmen gestoppt zu werden
  - nein...Weniger erfolgreiche Manipulation, ohne von Gegenmaßnahmen gestoppt zu werden

3.4 Auswertung: Manipulationsarten

Einzelne:

Manipulationsart	Zugang	Vollautomatisch	Zuverlässigkeit
IP	schwer	ja	ja
Vertraulichkeit	normal	ja	ja
Cookie	einfach	ja	nein
E-Mail	normal	ja	nein
CAPTCHA	schwer	ja	nein
Social Engineering	schwer	nein	ja

Gruppe:

Manipulationsart	Arbeitsaufwand Master	Verbreitung	Zuverlässigkeit
Online-Community	einfach	einfach	ja
Botnetz	schwer	einfach	ja

Tabelle 3: Auswertung: Evaluierte Manipulationsarten

Der Versuch einheitliche Kriterien zur Bewertung zu wählen wurde unternommen, um ein möglichst aussagekräftiges Endergebnis zu erhalten. Wie den vorliegenden Ergebnissen zu entnehmen, ist es auf Grund der Beschaffenheit der Manipulationsarten nicht gänzlich möglich.

An dieser Stelle soll kein Vergleich zwischen Einzel- und Gruppenmanipulationsarten dargestellt werden, sondern der allgemeingültige Kern der Manipulation. Der Einzelne hat generell das Potential hohen Schaden anzurichten, jedoch zumeist mit steigender Expertise im technischen Bereich, so dass der Anschluss des Einzelnen an eine Gruppe beziehungsweise das Agieren von vielen Einzelnen als Gruppe mit höherer Zuverlässigkeit zur Manipulation führt. Es kann keine allgemeingültige Aussage gegeben werden, die bestimmt, ob eine bestimmte Manipulation zu gegebenen Bedingungen erfolgreich zum Ziel führt, da sie von zu vielen Faktoren abhängt. Es existiert kein Katalog, wie ein bestimmtes Manipulationsziel erreicht werden kann. Hingegen kann die Aussage getroffen werden, aufgrund der bereits gegebenen Praxisbeispiele der Gruppe Anonymous (Kapitel 3.2.1 & 3.2.2) und allgemeiner Beschreibungen von Gruppenmanipulationsarten (Kapitel 3.1 & 3.2), dass die Manipulation in der Gruppe für den Einzelnen ohne technische Kompetenzen lukrativer ist, da er auf das Wissen der Gruppe (Vorarbeit des Masters, Kapitel 3.3) zurückgreifen kann und im Bereich Botnetz lediglich seinen eigenen PC zur Verfügung stellen muss (Slave, Kapitel 3.3).

4 Ergebnisse und Diskussion

Die vorliegende Arbeit erläutert das breite Themenumfeld der Manipulationsmöglichkeiten bei Online-Votings, analysiert Probleme und leitet daraus Zielstellungen ab. Anhand der Gegenüberstellung Manipulation als Einzelner oder Gruppe wurde die allgemeine Manipulation beschrieben, durch ein aus der Praxis entnommenen aktuellen Beispiels untersetzt sowie evaluiert und verglichen. In Form einer Breitenanalyse wurden Manipulationsmöglichkeiten und Gegenmaßnahmen evaluiert. Die Tabelle über Manipulationsarten aus dem vorhergehenden Abschnitt zieht ein weiteres Resümee zu den Ergebnissen im Abschnitt 2.3 und 3.3. Ausgehend vom regulären Benutzer ist zu erkennen, dass die gezeigten Manipulationsarten manuell ausgeführt, jedoch in ihrer Vollständigkeit komplett vom Computer übernommen werden können. Substituiert man den regulären Benutzer mit einem Computer und stellt sich ein Netzwerk aus mehreren Computern vor, so erhält man ein Botnetzwerk, welches lediglich die Aufgabe der Manipulation erfüllen soll. Abstrahiert man vom Botnetzwerk auf Online-Communities erhält man ähnliche Resultate durch den Einsatz mehrerer Menschen.

Die hier versuchte Trennung der einzelnen Manipulationsarten und deren Gegenmaßnahmen wird im praktischen Einsatz meist in Kombination mehrerer Gegenmaßnahmen realisiert. Das heißt, sowohl IP-Adress-Filterung, als auch CAPTCHA Authentifizierung kommen meist kombiniert zum Einsatz. Die eingesetzte Manipulationsart im Bereich der Gruppen ist zumeist nicht so klar zu trennen, beziehungsweise zu erkennen. Der Online-Votingbetreiber steht meist nur vor einer Masse von Anfragen (HTTP-request)[50] von verschiedenen IP-Adresse, die nicht darüber Aufschluss geben, ob es sich um ein Botnetzwerk oder eine Online-Community handelt, bei der eine hohe Anzahl an berechtigten Umfrageteilnehmern abstimmt.

Wie der vorhergehenden Tabelle als Quintessenz zu entnehmen ist, stehen Betreiber von Online-Votings einer Manipulation durch Gruppen nahezu machtlos gegenüber, wenn sie das Online-Voting der Masse zur Verfügung stellen wollen. Durch Personifizierung der einzelnen Online-Votings, durch Angabe persönlicher Daten, Logins, E-Mailbestätigung usw. ist die Aussagekraft durch Schwinden der Quantität im Bereich Teilnahme gefährdet. Diesen Prozess will der reguläre Benutzer nicht bestreiten, dem dadurch der einfache Zugang zur Teilnahme erschwert wird.

[50] HTTP: Hypertext Transfer Protocol - Ein Kommunikationsschema zum Austausch von Daten im Internet.

Die Anspruchshaltung in Form der Zielstellung wurde konsequent umgesetzt und resultiert in der Aussage: *Online-Votings sind nicht repräsentativ*, weil die Manipulationsmöglichkeiten zu vielfältig, einfach umsetzbar, teils voll automatisierbar und deren Gegenmaßnahmen zur Erhöhung der Sicherheit oft mit Unannehmlichkeiten für den Benutzer in Form von verlängerten Anmeldeprozessen, Eingabe von CAPTCHA-Codes etc. verbunden sind und diese trotz dessen manipulierbar bleiben.

5 Perspektive

Die Recherche hat ergeben, dass es in dem gewählten Themenumfeld ein Mangel an Publikationen gibt. Damit erklärt sich der Neuigkeitswert dieser Arbeit in dem gegebenen Überblick sowie den Ergebnissen. Damit hat das Thema der Arbeit Potential aktueller Forschungsgegenstand zu werden und liefert eine Vorlage für eine detaillierte Tiefendarstellung der einzelnen Themen aus den Kapiteln 2.2 und 3.2.

Die vorliegende Arbeit, als Grundlage für weiterführende Studien, an der Hochschule Mittweida, ist im Bereich: Durchführung Schein-Online-Voting geeignet. Ein mögliches Szenario wäre die Erhebung über die tatsächlich eingesetzten Manipulationen dieses Votings, das speziell darauf präpariert wurde, Angriffsfläche zu bieten durch den Einsatz von beispielsweise CAPTCHA Authentifizierungen usw.. Mit der daraus abgeleiteten Statistik können anschließend Aussagen zur IT-Security der Hochschule getroffen werden. Die Hochschule in ihrer Rolle als Vorbild kann dann gezielter IT-Security-Awareness, das Bewusstsein für IT-Sicherheit ausbilden.

Literatur

[1] 24HTRICKSTER: Operation Pril. In: *http://www.24htrickster.net/wbb/small-talk/17760-operation-pril/ [Stand: 10.07.12]*

[2] BAYER, C. : Anonyme E-Mailadressen ohne Anmeldung. In: *www.trash-mail.com [Stand: 01.07.12]*

[3] BREITHUT, J. : Pril-Wettbewerb endet im PR-Debakel. In: *http://www.spiegel.de/netzwelt/netzpolitik/soziale-netzwerke-pril-wettbewerb-endet-im-pr-debakel-a-763808.html [Stand: 11.07.12]*

[4] CHRISTL, A. : *Cookies, Web-Logs, Location Based Services, eMail, Webbugs, Spyware- Datenschutz im Internet*. GRIN Verlag GmbH, 2008. – ISBN 9783640221103. – S. 7, 126

[5] COMPUTERWORLD: *Lexikon: Aktuelle Fachbegriffe aus Informatik und Telekommunikation*. Vdf Hochschulverlag AG, 2007 (Computerworld-Lexikon). – ISBN 9783728131089. – S. 32

[6] EIKENBERG, R. : Windows Update kompromittiert. In: *http://www.heise.de/security/meldung/Windows-Update-kompromittiert-1605393.html [01.07.12]*

[7] FESTIVAL-TEAM: Wer soll Mittweida rocken? Manipulation beim Onlinevoting und seine Konsequenzen. In: *http://www.global.hs-mittweida.de/ cf/wordpress/ [Stand: 02.05.12]*

[8] FINSTER, D. : *Online Communities: Geschäftsmodelle unter dem Einfluss des Electronic Commerce*. Diplomica Verlag, 2011. – ISBN 9783842861954. – S. 19

[9] FREEBIES: Fight with Spam: 15+ Free Captcha Solutions. In: *http://www.1stwebdesigner.com/freebies/captcha-solutions-kill-spam/ [Stand: 01.07.12]*

[10] FUEHRER, D. : Anonyme E-Mailadressen ohne Anmeldung. In: *www.trashmail.de [Stand: 10.07.12]*

[11] HILLARD, D. : Temporäre E-Mailadressen ohne Anmeldung. In: *www.10minutemail.com [Stand: 10.07.12]*

[12] ISRAEL, T. : Teammeeting. In: *http://www.doodle.com/5ypkegwmd8m23ykntable [Stand: 11.05.12]*

[13] KNILL, M. : Beeinflussung-Manipulation-Propaganda. In: *http://www.rhetorik.ch/Beeinflussen/Beeinflussen.html [Stand: 02.05.12]*

[14] LAMERE, P. : Inside the precision hack. In: *http://musicmachinery.com/2009/04/15/inside-the-precision-hack/ [Stand: 01.07.12]*

[15] LAMERE, P. : moot wins, Time Inc. loses. In: *http://musicmachinery.com/2009/04/27/moot-wins-time-inc-loses/ [Stand: 01.07.12]*

[16] LECKER, R. : Die Causa Pril und andere Social Media Problemchen. In: *http://robertlecker.wordpress.com/2011/05/18/die-causa-pril-und-andere-social-media-problemchen/ [Stand: 01.07.12]*

[17] LIPSKI, M. : *Social Engineering - Der Mensch als Sicherheitsrisiko in der IT*. Diplomica Verlag, 2009. – ISBN 9783836675741. – S. 7-9

[18] LOCHMAIER, L. : Risikofaktor Mensch: Die Kunst des Social Engineering. In: *http://www.zdnet.de/magazin/39152145/risikofaktor-mensch-die-kunst-des-social-engineering.htm [Stand: 01.07.12]*

[19] MARQUARD, J. : Deutsche eSport-Seite mit aktivem Forum. In: *www.readmore.de [Stand: 01.07.12]*

[20] MITNICK, K. ; SIMON, W. ; DUBAU, J. : *Die Kunst der Täuschung: Risikofaktor Mensch*. mitp-Verlag, 2006. – ISBN 9783826615696. – S. 20

[21] MOOT, C. : Internationale Website mit aktivem Forum. In: *www.4chan.org [Stand: 01.07.12]*

[22] MORAWE, R. : *Spam- Prävention und Bekämpfung*. GRIN Verlag, 2009. – ISBN 9783640412068. – S. 14,15

[23] PAULH: Bandvoting, need Help! In: *http://www.readmore.de/index.php?cont=forum/thread&threadid=89303&page=1 [Stand: 01.07.12]*

[24] PLANETSHAKER: Wie Anhänger von Wikileaks gegnerische Server sabotieren. In: *http://www.planetshaker.de/wp-content/uploads/2010/12/Loic1.jpg [Stand: 01.07.12]*

[25] REISSMANN, O. ; STÖCKER, C. ; LISCHKA, K. : *We are Anonymous: Die Maske des Protests - Wer sie sind, was sie antreibt, was sie wollen*. E-Books der Verlagsgruppe Random House GmbH, 2012. – ISBN 9783641083748. – S. 5, 39-41, 71

[26] SCHMITT, I. : *Der Computer als Vermittler zwischen Mensch und Mensch.* GRIN Verlag GmbH, 2010. – ISBN 9783640609932. – S. 3

[27] STUDER, B. : *Netzwerkmanagement und Netzwerksicherheit: Ein Kompaktkurs für Praxis und Lehre*. Vdf Hochschulverlag AG, 2010 (Vdf Praxis und Lehre). – ISBN 9783728133199. – S. 110

[28] WAGNER, D. : *IT- Security: Aktuelle Angriffs- und Abwehrmethoden: Botnetze*. GRIN Verlag, 2011. – ISBN 9783640935611. – S. 27

[29] WARD, J. R.: History of Pen and Gesture Computing. In: *http://rwservices.no-ip.info:81/pens/biblio90.html [Stand: 03.05.12]*

[30] WEISS, C. : *Bewertung von Online-Communitys- Ein ökonomischer Ansatz und seine Anwendung am Beispiel der XING AG*. GRIN Verlag GmbH, 2008. – ISBN 9783640224418. – S. 23

Eigenständigkeitserklärung

Hiermit erkläre ich, dass ich die vorliegende Arbeit selbstständig und nur unter Verwendung der angegebenen Literatur und Hilfsmittel angefertigt habe. Stellen, die wörtlich oder sinngemäß aus Quellen entnommen wurden, sind als solche kenntlich gemacht. Diese Arbeit wurde in gleicher oder ähnlicher Form noch keiner anderen Prüfungsbehörde vorgelegt.

Ort, Datum Vorname Nachname